EPC Newsletter

SEPA FOR CARDS

Work in Progress

The EPC approves update of the SEPA Cards Standardisation Volume and a new Resolution 'Preventing Card Fraud in a Mature EMV Environment'

31.01.11 BY UGO BECHIS AND CÉDRIC SARAZIN

In December 2010, the European Payments Council (EPC) approved version 5.0 of the SEPA Cards Standardisation Volume - Book of Requirements taking into consideration that chapters 5 (security requirements) and 6 (certification) are subject to further amendments. The Standardisation Volume defines functional and security standards requirements as well as an evaluation methodology designed to achieve interoperability based on open and free standards within SEPA. Also in December 2010, the EPC approved the Resolution 'Preventing Card Fraud in a Mature EMV Environment'. Both documents, together with the SEPA Cards Framework, are key deliverables of the EPC designed to promote the creation of a SEPA for Cards. Ugo Bechis and Cédric Sarazin report in detail on the new elements incorporated into the SEPA Cards Standardisation Volume - Book of Requirements and identify the appropriate measures to fight fraud in a mature chip and PIN card ecosystem as set out in the related EPC Resolution.

KEY INFORMATION IN THIS ARTICLE

Version 5.0 of the SEPA Cards Standardisation Volume – Book of Requirements (BoR) includes the following new elements:

- Chapter 3: new references to EMV and mobile payments related documentation and several new definitions have been added to this section: ‘acceptance environments’; ‘Attended’ environments and ‘Unattended Non PIN’ environments, ‘Acceptance Environments for Remote Transactions’.
- Chapter 4 (functional scope and requirements) now includes additional functional requirements applicable to transactions initiated by a card such as ‘Cards Services’, ‘Acceptance Technologies’, ‘Acceptance Environments’, ‘Cardholder Verification Methods’. In scope are now ATM cash withdrawal transactions, ‘Chip Contactless EMV Based’ technologies, ‘Contactless with Mobile’ technologies, ‘Unattended non PIN Acceptance Environment’ and the usage of ‘Mobile Code for Card Authentication'.
- Chapter 5 (security requirements) has been updated to cover both cards and terminal requirements, however, this chapter is subject to further consultation.
- Chapter 6 (certification) remains unchanged compared to version 4.0 of the Standardisation Volume – BoR published in December 2009. The future version of chapter 6 will reflect the results of the ongoing discussions between the EPC and CAS on the adoption of a European Certification framework and the set up of the European Certification Body.

The EPC Resolution ‘Preventing Card Fraud in a Mature EMV Environment’ defines measures to achieve the following objectives:

- Limit the potential impact of an incomplete migration to EMV outside SEPA on SEPA issuing
- Reducing fraud in card-not-present environments
- Protection of payment data, notably from data compromise.

A brief overview of EPC deliverables in the area of cards

The EPC has developed the SEPA Cards Framework (SCF). The aim of the SCF is to enable a consistent customer experience when making or accepting payments and cash withdrawals in euros with cards that have achieved a very high levels of security. The SCF outlines high level principles and rules that when implemented by the card industry will deliver this consistent user experience to both cardholders and merchants.

The objectives of a SEPA for Cards will be achieved to the greatest extent possible through the use of open and free standards available to all parties within the card payment value chain. The EPC is carrying out a cards standardisation programme designed to remove technical obstacles preventing a consistent customer experience throughout the SEPA cards market and to allow a higher process efficiency along the overall card chain. In 2009, the EPC promoted the creation of the Cards Stakeholders Group (CSG) together with representatives of five sectors also active in the cards domain including retailers, vendors - such as manufacturer of card payment devices and related IT systems, processors, card schemes and banks.

Creating this body makes it possible to pinpoint the expectations of a broad range of stakeholders while ensuring a strong co-management in the process of identifying standards requirements and implementation best practices that will promote interoperability in the SEPA cards market. The CSG develops the SEPA Cards Standardisation Volume - Book of Requirements (BoR) which defines the functional and security standards requirements as well as an evaluation methodology designed to achieve interoperability based on open and free standards within SEPA.

Last but certainly not least, card fraud prevention is a top priority of the EPC.

The EPC Card Fraud Prevention Task Force was established in 2003, and from the very beginning included non-bank stakeholders. It was also at this time that the EPC committed to migrate all SEPA cards and terminals to chip and PIN (personal identification number) based on the global EMV standards by the end of 2010 [1]. Nearing the completion of this migration, the EPC Card Fraud Prevention Task Force now focuses on identifying and promoting measures to fight card fraud in a mature chip and PIN environment.

The EPC approves version 5.0 (chapters 1 - 4) of the SEPA Cards Standardisation Volume - BoR - further work on chapters 5 and 6 remains in progress

In December 2010, following the positive review by the CSG, the EPC approved version 5.0 of the Standardisation Volume - BoR for publication with qualifications regarding chapters 5 and 6 and acknowledging that a future update will be considered in the course of 2011. Approval of chapters 5 (security requirements) and 6 (certification) was deferred pending additional changes.

Changes incorporated into version 5.0 of the Standardisation Volume - BoR compared to version 4.0

Chapter 3 of the Standardisation Volume - BoR contains references, abbreviations and definitions. Changes to this section include new references to EMV and mobile payments related documentation as well as new abbreviations related to mobile payments. In addition, several new definitions have been added to this section. For example definitions on 'acceptance environments' describe the various environments in which a card payment may take place such as 'attended' environments (a situation where the transaction occurs 'face-to-face') or 'unattended non-PIN' environments (situations such as parking meters or highway tolls). Definitions on 'acceptance environments for remote transactions' specify types of payments made where the cardholder is neither physically present at the acceptor nor at an unattended terminal, as is the case when payments are made online.

Chapter 4 (functional scope and requirements) now includes additional functional requirements applicable to card transactions. The subsections of this chapter were updated to include 'Cards Services' (the types of transactions), 'Acceptance Technologies' (how the card is read), 'Acceptance Environments' (where the transaction is made), and 'Cardholder Verification Methods' (how the transaction is verified, i.e. PIN or signature). The specific items focused on are ATM cash withdrawal transactions as well as 'chip contactless EMV based' technologies and 'contactless with mobile' technologies. In addition, the 'unattended non-PIN acceptance environment' and the usage of 'mobile code for card authentication' are covered. Descriptions and diagrams related to these items were adapted accordingly. The functional requirements were adjusted to reflect these changes.

Chapter 5 (security requirements) has been updated to cover both card and terminal requirements, however, this chapter is subject to further amendments resulting from consultation of stakeholders. With regard to the amendments that have been made, this chapter now includes a section on 'Security Objectives' covering, specifically, 'transaction protection', 'smartcard', 'user authentication', 'execution protection' (how the card enforces protection of its services), 'data protection', and 'services protection' (how the card enforces its own security to protect its services).

A new section titled 'Assurance Level' describes the evaluation methodology designed to provide assurance of a product's security properties. Last but not least, chapter 5 outlines the 'EPC Security Requirements'. These requirements are based on PCI POS PED 2.0 developed by the Payment Cards Industry Security Standards Council[2] and have been extended to address the perceived threats and vulnerabilities of European markets. These 'EPC Plus' requirements include, as targets for evaluation, further elements impacting the point of interaction such as secure software download, privacy shielding, local input and output of data, application separation, and support for secure communications of data with external entities like an acquirer and code review.

Chapter 6 (certification) remains unchanged compared to version 4.0 of the Standardisation Volume - BoR published in December 2009.

Currently, cards and terminals need to be certified for each market and card scheme subject to different criteria and procedures. To-date, the certification of cards and terminals takes place based on requirements also defined at a national level. Moving forward, the goal is to establish a European certification framework enabling the manufacturers of cards and terminals to obtain a single certification that is recognised in all 32 SEPA countries. Thus by having a standard SEPA certification process, vendors can take advantage of greater economies of scale. To this end, considerations are underway to create a 'European Certification Body'.

The future version of chapter 6 will reflect the results of the ongoing joint work between the EPC and CAS on the adoption of a European Certification Framework and the establishment of the European Certification Body. The design of the architecture (certification framework) allowing for the trusted and common security and functional evaluation and certification of cards and terminals at a SEPA level is essential to cater to the needs of more than 500 million cardholders and millions of merchants. The SEPA cards and terminal certification framework will ensure that any card or terminal certified by an accredited body can be deployed and used anywhere throughout SEPA.

EPC Resolution on card fraud prevention in a mature chip and PIN environment

In December 2010, the EPC also approved the Resolution 'Preventing Card Fraud in a Mature EMV Environment'. At the end of the third quarter of 2010, EMV compliance was 79 percent for cards, 95 percent for POS (points of sale) and 95 percent for ATMs.

The following trends can be observed in the mature chip and PIN environment:

- Card fraud prevention as such represents a major financial and operational cost saving opportunity for banks.
- The situation is considered to be under control when the card is present and the chip can be used (in face-to-face payments and cash withdrawals).
- Fraud is migrating rapidly to points of least resistance, i.e. non-chip countries outside SEPA based on the fraudulent use of magnetic stripes on cards which have been previously 'skimmed' (i.e. copied) by fraudsters.
- Instances of card-not-present fraud (i.e. card payments in e-commerce, by telephone or mail order) are increasing and represent up to 70 percent of the total fraud in some systems.

The EPC's Resolution 'Preventing Card Fraud in a Mature EMV Environment' identifies the following measures to fight fraud in a mature chip and PIN card ecosystem.

Limiting the potential impact of an incomplete migration to EMV outside SEPA on SEPA issuing

Through cross-regional liability shifts[3], global schemes should ensure that SEPA issuers and acquirers are shielded from any negative impact of an absent or incomplete global migration to EMV outside SEPA. For markets that have started their plans for a mature EMV environment, the implementation of the liability shift within non-SEPA markets should be effective by 2015 at the latest.

For non-SEPA markets, the implementation of this Resolution would also benefit from the persuasion power of European regulators such as the European Central Bank (ECB) and the European Commission and the action of European banks with global presence.

The EMV chip environment is key to ensure security and fraud protection. The EPC Resolution calls additionally for restriction of magnetic stripe fallback and the option to adopt chip only issuing.

The EPC therefore reaffirms its statement on magnetic stripe fallbacks[4]: card schemes should aim to restrict the use of magnetic stripe fallback to exceptional cases (without of course putting at risk business continuity requirements, or compromising card issuers ultimate right to accept fallback transactions). PAN key entry as a fallback should be prohibited[5].

Finally, the EPC expects that SEPA card schemes grant issuers the option to adopt a chip-only approach, be it by issuing chip only cards or by allowing them to refuse magnetic stripe transactions if they so wish, providing that there is clear and formal communication to the cardholder.

Reducing fraud in card-not-present environments (e-Commerce and orders by mail or telephone)

The EPC recommends that cards schemes and their members implement within SEPA the following measures:

E-commerce on the issuing side: issuers and card schemes shall provide evidence at the latest **by end 2013** that appropriate authentication solutions are in place. Such solutions should be interoperable between schemes to avoid acceptance barriers. These could be harmonised based on authentication methods used for online banking. Such authentication solutions could be:

- Risk-based authentication
- Challenge-response mechanism
- Dual channel authentication such as SMS
- Hardware based authentication such as a token or chip reader
- Virtual cards
- Or any innovative solutions considered effective by payment schemes.

These authentication methods should be combined with appropriate risk management tools.

E-commerce on the acquiring side: card schemes will have to provide evidence at the latest **by end 2013** that they are able to support such authentication solutions on the acquiring side.

Mandatory usage of 'CVX2'[6] in all card-not-present environments: from 1 January 2012 onwards, card schemes will have to mandate at a minimum that in all card-not-present environments, and for cards capable of transactions in such environments

- Acquirers have to acquire and transmit 'CVX2' values or their equivalent.
- Issuers have to decline any authorisation request made with a false 'CVX2' value or its equivalent ('CVX2 mismatch').

For *recurring* payment transactions, where the merchant has stored the card number and the expiry date but not the 'CVX2' or its equivalent, the presence of the 'CVX2' value is only required for the initial transaction.

An exception applies for merchants having implemented or submitted plans to acquirers to comply with the above listed authentication mechanisms listed above with regard to e-commerce on the acquiring side.

Card schemes may also allow exceptions or temporary waivers for specific, low-fraud sectors, as long as these represent less than 10 percent of the SEPA acceptance basis.

For environments not responding to waivers, issuers should be advised to decline any authorisation request not carrying a 'CVX2' value or its equivalent ('CVX2 missing').

The main objective of the usage of 'CVX2' or its equivalent is to prevent cross-contamination (i.e. the reuse in card-not-present environments of data potentially compromised in chip / magstripe cardpresent environments). This is achieved by requiring the presence of a data element (the 'CVX2' or its equivalent) which is not present in other card-present environments (chip or magstripe transactions).

Protection of payment data, notably from data compromise

As a general principle, the storage or the transportation of sensitive data in a secure way should be limited to data strictly necessary to handle cards transactions. The EPC will consider endorsement of Data Security Standards (DSS), and promote use of DSS among the members of the CSG. The CSG will be invited to deliver its view on migration to DSS.

In such a migration plan, data protection (e.g. encryption) efforts should focus on sensitive card data that could be misused for card transactions. These efforts should capitalise on a risk based approach and take into consideration EMV migration. Measures should be put in place to make the use of compromised data difficult (e.g. dynamic EMV and 'eCVx' based transactions or end-to-end data encryption). 'Sensitive data' will be defined in the Standardisation Volume - BoR. To that end, EPC will cooperate with the relevant stakeholders to include data protection or encryption requirements in the Standardisation Volume - BoR, agree on a European approach on data security standards and increase European influence in global organisations (e.g. PCI SSC).

As regards standard implementation, the recommendation to use 'CVX2' or an equivalent for all card-not-present transactions should be considered as a priority to avoid cross contamination between secure and non-secure environments (see above). Consequently, DSS should only be mandated when sensitive data is stored or not protected and should only be enforced on a risk-based prioritised approach keeping in mind the reduced risk inherent to EMV.

Next steps

Following the successful implementation of chip and PIN in Europe and all its beneficial effects on card fraud reduction, the EPC has taken the necessary decisions to contain the increase of fraud in non-chip environments. In 2011, the EPC Cards Working Group will analyse further measures to effectively fight card fraud. The EPC Resolution 'Preventing Card Fraud in a Mature EMV Environment' could be reflected in other card reference documents and also, potentially, new voluntary measures such as the neutralisation of magnetic stripes on European cards might be considered.

This approach is in line with a further priority of the EPC's activities in the area of cards; i.e. to ensure consistency of the SCF and the Standardisation Volume - BoR as well as the related implementation specifications developed by relevant standardisation initiatives. The SCF and the Standardisation Volume - BoR are both aimed at setting the conditions for a better, more cost efficient and richer card services and product offer, whatever the card product or scheme may be. It is up to schemes and banks to take advantage from these improved conditions to the benefit of the overall market, the customers first and all the card stakeholders.

Ugo Bechis is the Chair of the EPC Cards Working Group. Cédric Sarazin is the Chair of the EPC Card Fraud Prevention Task Force.

Related links:

EPC Resolution 'Preventing Card Fraud in a Mature EMV Environment'

SEPA Cards Framework

SEPA Cards Standardisation Volume (version 5.0)

Related article in previous issue:

New Business Opportunities with Chip and PIN. How to create added value based on EMV technology (EPC Newsletter, Issue 7, July 2010).

[1] The EPC's SEPA Cards Framework (SCF) recognises the EMV standard for SEPA-wide acceptance of payments with cards at very high levels of security. EMV is an industry standard to implement chip and PIN security for card transactions.

[2] For more information on PCI SSC visit https://www.pcisecuritystandards.org/about/index.shtml

[3] EMV liability shifts are interbank scheme rules which put the financial responsibility in case of fraud on the party which did not invest in the EMV chip card or terminal.

[4] Magnetic stripe fallbacks are used in case the payment terminal would have a problem to process the transaction with the chip of the card. This consists of going back to the magnetic stripe type of transaction. This possibility is sometimes used by fraudsters who want to exploit the weaknesses of the magnetic stripe even on chip cards.

[5] PAN key entry occurs as a fallback when a magnetic stripe or a chip cannot be read. To complete a PAN key-entry transaction, only the PAN, expiration date, and customer signature are necessary, making this technique easily susceptible to fraud from cardholder data compromised in any acceptance channel. While PAN key entry requires the forgery of the cardholder signature, this method of cardholder verification is potentially less reliable as it may be either incorrectly verified by a merchant or simply not checked. This method of data entry is restricted, controlled, and used infrequently in a mature EMV environment, thus limiting PAN key-entry fraud. (PCI DSS Applicability in an EMV Environment - A Guidance Document, October 2010 © 2010 PCI Security Standards Council, LLC

[6] The 'CVX2' is a set of 3 or 4 numbers printed on the back of the cards which are requested from the cardholder when he does a transaction on the internet or over the phone. These numbers not being present in magnetic stripe or chip transaction data, if the 'CVX2' were mandated for all card-not-present transactions, would stop fraudsters who capture data in a card-present environment and try to use the card to make fraudulent payments in card-not-present environments.

ARTICLE164